IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF RICHARD A. DeMILLO

RICHARD A. DeMILLO ("Declarant") hereby declares as follows:

1. I am a registered voter in Fulton County Georgia. I am deeply interested in the proper functioning of the Georgia's voting system, from both a personal and professional perspective.

2. I am currently the Charlotte B. and Roger C. Warren Chair of Computer Science at Georgia Tech. I have served as Dean of the College of Computing at Georgia Tech and Director of the Georgia Tech Center for Information Security. I have also served as the Chief Technology Officer for Hewlett-Packard, Vice President and General Manager of Computing and Information Research at Bell Communications Research, Director of the Computer

and Communications Research Division at the National Science Foundation, and Director of the Software Test and Evaluation Project for the U.S. Department of Defense. In all these appointments, my primary technology focus has been information, communication, and cyber security and computer system testing. I have taught both graduate and undergraduate courses in cyber security, supervised graduate students, and conducted peer-reviewed research leading to journal articles, patents, and invited addresses, all related to the topic of cyber threats to computer systems.

3. A copy of my cv is attached as Exhibit 1.

4. I am familiar with Georgia’s Diebold DRE voting system, its design, the body of academic literature compiled on the system in the last ten years, and its operation as it is deployed in the polling places in Georgia.

5. I own Diebold TSx and TS voting machines purchased over e-Bay which I have examined and used to conduct certain experiments related to the DRE system security. Over the past year, I have conferred with many colleagues in the field of cyber security, including Matthew Bernhard and Logan Lamb who have sought my technical input for their research into Georgia’s DRE voting system.

6. I have observed the operation of the Diebold DRE system in polling places in multiple Georgia counties over the course of multiple elections and in county election offices where the system was being programmed and tested. I have

observed the testing procedures conducted prior to machine deployment to the polling places.

7. I have also observed the Diebold DRE voting machines being hacked in demonstrations, most recently in a public seminar at Georgia Tech in April 2018.

8. I am not a retained expert by any party to this action, but in the desire to aid the Court in the evaluation of the Defendant's assertions, I wish to voluntarily offer my opinion on one topic included in the State Defendant's response brief [Doc. 265, page 3]

9. In summary, Defendants' briefs and supporting declarations show a lack of basic understanding of the nature of current cybersecurity attacks being used against the nation's election systems and commercial systems. Defendants do not appear to understand the most basic realistic threats to the state's election system which may have already altered the operation of the system in undetected ways.

10. Defendants ridicule Coalition Plaintiffs, stating, "'Undetectable manipulation' is Plaintiffs' phrase de jure for the convenient reason that it dodges any test for corroboration. Evidence of 'undetectable manipulation' is oxymoronic."

11. Defendants assert that Plaintiffs have concocted the idea of undetectable manipulation to suit the needs of the present lawsuit. This is a false assertion. Undetectable manipulation is the most common, widely recognized, and serious threat facing computer systems, including election systems. Techniques for undetectable manipulation, methods for counteracting the threats, and the capabilities that are needed to mount a successful defense to such attacks are defined by the National Institute of Standards and Technology (NIST) and are contained in the standard curriculum in virtually every university level course on cyber security. Furthermore, as the following citations show, the threat is not speculative or theoretical but rather is the fundamental building block of modern cyber security and cyber warfighting.

12. Undetectable manipulation is a standard behavior of Advanced Persistent Threats[1] or APT, the threats that the US Intelligence Agencies have determined with high confidence attacked US election systems in 2016 and continue to attack the mid-term elections[2]. According to NIST, "The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of

[1] National Institute of Standards and Technology, https://csrc.nist.gov/Glossary/?term=2856

[2] https://www.burr.senate.gov/press/releases/senate-intel-committee-releases-unclassified-1st-installment-in-russia-report-updated-recommendations-on-election-security

time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives."[3] Attacks due to APTs are mounted by state and nonstate actors and constitute one of the principle attack vectors for modern cyberwarfare.[4]

13. There is ample publicly disclosed cause to believe[5] that US election systems (including Georgia's) have been subject to APT attacks that yield undetectable manipulation. APTs use exactly the attacks that have been documented in classified and unclassified analyses of Russian activities[6] to disrupt and hack US election systems[7] "A persistent attack will probe networks, scour social networks for information they can find about the target's employee and perform other analysis and reconnaissance. Any organization that does not think they enough value to motivate a criminal to be persistent should be out of business."[8]

14. One characteristic of attacks mounted by APTs is that they can evade detection by doing damage before IT managers, antivirus companies, and

[3] National Institute of Standards and Technology https://csrc.nist.gov/Glossary/?term=2856
[4] Jeffrey Carr, Inside Cyberwarfare, O'Reilly Publishers, 2009. P.119
[5] https://www.justice.gov/file/1080281/download
[6] ibid
[7] https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1
[8] Ira Winkler APT Security, p. 39

hardware/software vendors are aware that an attack has taken place: “If a virus can infect 10 million computers...in the hours before a fix is released, that’s a lot of damage. What if the code took pains to hide itself, so that a virus wasn’t discovered for a couple of days? What if [a] worm just targeted an individual, and deleted itself before off any computer whose userID didn’t match a certain reference?”[9]

15. Current textbooks on methods for subverting operating systems, answer these questions in great detail and should be well-known to election officials who operate the computer systems that are targeted by APTs: “A back door in a computer is a secret way to get access….They are very real…To remain undetected a back-door program must use stealth…Professional attack operations usually require specific and automated back door programs—programs that do only one thing and nothing else. This provides assurance of consistent results.”[10] The software that installs these back-door programs and then erases all evidence of its existence is called a Rootkit.

16. There are catalogs of viruses and other programs that install Rootkits. These catalogs are studied by undergraduate computer science students to prepare

[9] Bruce Schneier, Secrets and Lies: Digital Security in a Networked World,” John Wiley & Sons, 2000 p. 158

[10] Greg Hoglund and James Butler, “Rootkits: Subverting the Windows Kernel,” Addison-Wesley, 2006 pp. 2–3

them to counter APTs in practice. Among these programs are Polymorphic Viruses: “These are the most difficult to detect. They have the ability to mutate, which means that they change the viral code known as the signature each time they spread or infect. Thus, antiviruses that look for specific virus codes are not able to detect such viruses.”[11]

17. Standard textbooks[12] list the many forms that a back door might take:

a. “Install an altered version of *login*, *telnetd*, *ftpd*, *rshd*, *inetd*, or some other program; the altered program usually accepts a special input sequence[13] and spawns a shell for the user.

b. Plant an entry in the *.rhosts*, *.shosts*, or *.ssh/authorized_keys* file of a user or the superuser to allow future unauthorized access.

c. Change the */etc/fstab* file on an NFS system to remove the *nosuid* designator, allowing a legitimate user to become *root* without authorization through a remote program.

[11] Ankit Fadia, “The Unofficial Guide to Ethical Hacking,” Premier Press, 2002 p. 434

[12] Simson Garfinkel, Gene Spafford, and Alan Schwartz, “Practical Unix & Internet Security (3rd edition), O’Reily Publishers, 2003

[13] This capability is one of the reasons experts are alarmed by unauditable bar codes in ballot marking devices. Such codes can embed such special input sequences.

d. Add an alias to the mail system so that when mail is sent to that alias, the mailer runs a program of the attacker's designation, possibly creating an entry into the system.

e. Change the owner of the /*etc* directory so the attacker can rename and subvert files such as the */etc/passwd* and /*etc/group* at a later time

f. Change the file permissions of /*dev/kmem* or your disk devices so they can be modified by someone other than *root*.

g. Change a shared library or loadable module to add a system call option to allow a change to superuser status when using a seemingly innocuous program,

h. Install a harmless-looking shell file somewhere that set SUID so a user can use the shell to become *root*.

i. Change or add a network service to provide a *root* shell to a remote user.

j. Add a back door to the *sshd* binary so that a specific username and password is always accepted for login, whether or not the username exists in the accounts database. Alternatively, the *sshd* binary might log all accepted usernames and passwords to a third-party machine.

Coupled with all of these changes, the attacker can modify timestamps, checksums, and audit programs so that the system administrator cannot detect the alteration!"[14]

18. Contrary to Defendants' claims that hackers "usually leave footprints," standard undergraduate cybersecurity textbooks describe how it is usual practice for APT attackers to cover their tracks and therefore not leave footprints:[15] "After an attack succeeds, most attackers immediately cover their tracks. Log files are adjusted, hacking tools are hidden, and back doors are installed, making future re-invasions simple. Rootkit has a number of tools to do this, and many others are out there. All hackers have tools to hide their presence. The most common tool is *rm*, and it is used on *syslog*, *utmp*, *utmpx* files."

19. Every computerized system in the Georgia Election System, including voter registration databases, employee and recruitment websites, network connected computers for provisioning systems of the kind located at the Kennesaw State University Center for Election Systems and which have now been transferred to the Office of the Secretary of State, Epollbooks used to provision voter cards on election day, servers used to provision ballot definitions on PCMCIA cards used in

[14] Garfinkel et al p. 738–739

[15] William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin, "Firewalls and Internet Security (Second Edition): Repelling the Wily Hacker," Addison-Wesley Professional Computing Series, 2003, pp. 126–127

Diebold voting terminals, the voting terminals themselves, GEMS servers and related software for tallying election night results, optical scanners used to process absentee and provisional ballots, and election night reporting systems all contain operating systems that are susceptible to the attack described above. Contrary to Defendants' assertions direct Internet access is not required to mount such attacks.[16]

20. As these citations make clear, undetectable manipulation is a grave threat to Georgia's paperless DRE voting system because APTs have plainly targeted the American election system, including in all likelihood Georgia's system. It is well within the capabilities and consistent with usual practice of those APTs to utilize undetectable manipulation. Given the inability of the State to determine with any certainty whether the software presently being utilized by Georgia's DRE voting system has been maliciously altered at any point in the past, it will be impossible for Georgians to have any reasonable degree of confidence in the integrity of the election results produced by Georgia's DRE voting system.

[16] Public demonstrations conducted by J. Alex Halderman in an open Seminar at Georgia Tech (April 16, 2018), witnessed by members of the public and legislative representatives from the Georgia House of Representatives and summarized for the general public in a New York Times article (https://www.nytimes.com/2018/04/05/opinion/election-voting-machine-hacking-russians.html). A written summary version of this experiment is being prepared for publication in technical journals.

Pursuant to 28 U.S.C. § 1746, I declare and verify under penalty of perjury that the foregoing is true and correct.

Executed on this date, August 20, 2018.

RICHARD A. DeMILLO